

17 MAR 1999

CHAPTER 9

TRANSMISSION AND TRANSPORTATION

9-1 BASIC POLICY

1. Commanding officers shall ensure that only appropriately cleared personnel or carriers transmit, transport, escort, or handcarry classified information. Unless a specific kind of transmission or transportation is restricted, the means selected should minimize the risk of a loss or compromise while permitting the use of the most cost-effective mode of conveyance.
2. All international transfers of classified information shall take place through government-to-government channels. Follow the provisions of exhibit 9A.

9-2 TOP SECRET

Transmit or transport U.S. Top Secret information only by:

1. Direct contact between appropriately cleared U.S. personnel;
2. The Defense Courier Service (DCS), if qualified under the provisions of reference (a);
3. The DOS Diplomatic Courier Service;
4. Communications protected by a cryptographic system authorized by the Director, NSA or a protected distribution system designed and installed to meet the requirements of reference (b). (This applies to voice, data, message, and facsimile transmissions);
5. Appropriately cleared DoD contractor employees or U.S. military or Government civilian personnel specifically designated to escort or handcarry the information, traveling on a conveyance owned, controlled, or chartered by the U.S. Government traveling by surface transportation;
6. Appropriately cleared U.S. military or Government civilian personnel, specifically designated to escort or handcarry classified information, traveling on scheduled commercial passenger aircraft within and between the U.S., its territories, and Canada;

17 MAR 1999

7. Appropriately cleared U.S. military and Government civilian personnel, specifically designated to escort or handcarry classified information, traveling on scheduled commercial passenger aircraft on flights outside the U.S., its territories, and Canada per paragraph 9-12; and

8. Appropriately cleared and designated DoD contractor employees within and between the U.S., its territories, and Canada per reference (c).

9-3 SECRET

Transmit or transport U.S. Secret information only by:

1. Any means approved for Top Secret information, except that Secret information may be introduced into the DCS only when U.S. control cannot otherwise be maintained. This restriction does not apply to COMSEC and SCI, per paragraph 9-5;

2. US Postal Service (USPS) registered mail within and between the U.S. and its territories;

3. USPS registered mail addressed to U.S. Government agencies through U.S. Army, Navy, Marine Corps, or Air Force Postal Service facilities outside the U.S. and its territories;

4. USPS and Canadian registered mail with registered mail receipt between U.S. Government and Canadian government installations in the U.S. and Canada;

5. USPS Express Mail sent between U.S. Government activities and cleared DoD contractors within and between the U.S. and its territories. Use USPS Express Mail Service only when it is the most cost effective way to meet program requirements. USPS Express Mail Service is strictly controlled in the DON and the official command mail control officer shall approve each use. The "Waiver of Signature and Indemnity" block on the USPS Express Mail Label 11-B shall not be executed under any circumstances. The use of external (street-side) Express Mail collection boxes is prohibited;

6. U.S. Government and Government contract vehicles including aircraft and ships of the U.S. Navy, civil service-operated U.S. Naval Ships (Military Sealift Command), and ships of U.S. registry. Appropriately cleared operators of vehicles, officers

17 MAR 1999

of ships, and pilots of aircraft who are U.S. citizens may be designated as escorts, provided the control and surveillance of the carrier is maintained on a 24-hour basis. The escort shall protect the shipment at all times through personal observation or authorized storage to prevent inspection, tampering, pilferage, or unauthorized access. Observation of the shipment is not required during flight or sea transit, provided it is loaded into a compartment that is not accessible to unauthorized persons or is in a specialized secure, safe-like container;

7. The current holder of the General Services Administration (GSA) contract for overnight delivery, when approved by the official command mail control officer. Use of this service is on an exception basis, when applicable postal regulations are met, and when an urgent requirement exists for overnight delivery for the executive branch to a DoD component or to a cleared DoD contractor facility within the U.S. and its territories. The delivery service shall be U.S.-owned and U.S.-operated, provide automated in-transit tracking, and ensure package integrity during transit. The contract shall require cooperation with U.S. Government inquiries in the event of a loss or possible compromise. Size and weight limitations shall be met. The sender shall ensure that an authorized person is available to receive the delivery and shall verify the correct mailing address. Under no circumstances shall the release signature block on the receipt label be executed. The use of external (street-side) collection boxes is prohibited. Classified COMSEC, NATO, and FGI shall not be transmitted in this manner;

8. Carriers cleared under the NISP who provide a Protective Security Service (PSS). This method is authorized only within the Continental U.S. (CONUS) when other methods are impractical, except that this method is also authorized between U.S. and Canadian government-approved locations documented in a transportation plan approved by the U.S. and Canadian government security authorities;

9. In the hold of a cleared U.S. registered air carrier (Civilian Reserve Air Fleet Participant) without an appropriately cleared escort, in exceptional circumstances with the written approval of the recipient government security authorities. The shipment shall be sent between two specific points with no intermediate stops. The carrier shall agree in advance to permit cleared and specifically authorized persons to observe placement and removal of the classified shipment from the air carrier. The shipment shall be placed in a compartment that is not accessible to unauthorized persons or shall be placed in the same type of specialized shipping container prescribed for use by the DCS.

17 MAR 1998

9-4 CONFIDENTIAL

Transmit or transport U.S. Confidential information only by:

- 1. Any means approved for Secret information;**
- 2. USPS registered mail to and from APO or FPO addressees located outside the U.S. and its territories, and when the originator is uncertain that the addressees location is within U.S. boundaries;**
- 3. USPS certified mail for information addressed to a cleared DoD contractor facility or non-DoD agencies;**
- 4. USPS first class mail between DoD component locations anywhere in the U.S. and its territories. The outer envelope or wrapper shall be endorsed: "RETURN SERVICE REQUESTED".**
- 5. A carrier that provides Constant Surveillance Service (CSS) within CONUS. A cleared DoD contractor facility shall be notified by separate communication at least 24 hours in advance of the shipment arrival. Information about commercial carriers providing a CSS is available from the Military Traffic Management Command (MTMC).**
- 6. Personal custody of commanders or masters of ships of U.S. registry who are U.S. citizens. Confidential information shipped on ships of U.S. registry shall not pass out of U.S. Government control. The commanders or masters shall receipt for the cargo and agree to:**
 - a. Deny access to the Confidential information by unauthorized persons, including customs inspectors, with the understanding that Confidential cargo that would be subject to customs inspections shall not be unloaded; and**
 - b. Maintain control of the cargo until a receipt is obtained from an authorized representative of the consignee.**

9-5 SPECIAL TYPES OF CLASSIFIED AND CONTROLLED UNCLASSIFIED INFORMATION

- 1. COMSEC. References (d) and (e) establish the requirements for the transmission or transportation of COMSEC information.**

17 MAR 1999

2. **NATO.** Reference (f) establishes the requirements for the transmission or transportation of classified NATO information. NATO RESTRICTED information shall, at a minimum, be transmitted by USPS first class mail within CONUS and USPS first class mail using an APO/FPO address outside CONUS (single wrapped). Geographical addresses and international mail channels shall not be used.
3. **SCI.** Reference (g) establishes the requirements for the transmission or transportation of SCI.
4. **SAPs.** Reference (h) establishes the requirements for the transmission or transportation of SAP information.
5. **SIOP and SIOP-ESI.** Reference (i) establishes the requirements for the transmission or transportation of SIOP and SIOP-ESI.
6. **NNPI.** The policies and procedures for the transmission or transportation of NNPI, U-NNPI, and DOE UCNI are contained in reference (l). Since there is foreign national access to the internet, U-NNPI may only be transmitted on the internet if the transmission is encrypted. The encryption standard for transmission of U-NNPI is Federal Information Processing Standards (FIPS) 140-1.
7. **RD (including CNWDI) and FRD.** Transmit or transport RD (including CNWDI) and FRD in the same manner as other classified information of the same security classification. Reference (j) establishes the requirements for the transmission or transportation of nuclear information or components.
8. **FOUO.** Transport FOUO information via USPS first class mail, or standard mail for bulk shipments. Electronic transmission of FOUO information (voice, data, or facsimile) shall be by approved secure communications systems whenever practical. All means used shall preclude unauthorized public disclosure per reference (k).
9. **SBU (formerly LOU).** Transmit or transport DOS SBU information in the same manner as FOUO information.
10. **DEA SENSITIVE INFORMATION.** Transmit or transport DEA Sensitive information within CONUS by USPS first class mail. Transmit or transport DEA Sensitive information outside the CONUS (double wrapped and marked on both sides of the inner envelope with "DEA Sensitive") by any means approved for the transmission

17 MAR 1999

or transportation of Secret material (see paragraph 9-3). Non-Government package delivery and courier services shall not be used. Electronic transmission of DEA Sensitive information within CONUS and outside CONUS shall be over approved secure communications circuits.

11. DoD UCNI. Transmit or transport DoD UCNI via USPS first class mail in a single, opaque envelope or wrapping. Except in emergencies, electronic transmission of DoD UCNI shall be over approved secure communications circuits per reference (m).

12. SENSITIVE INFORMATION (COMPUTER SECURITY ACT of 1987). Reference (n) establishes the requirements for the transmission of sensitive information in AISS.

13. FOREIGN GOVERNMENT RESTRICTED and UNCLASSIFIED INFORMATION PROVIDED IN CONFIDENCE. Transmit or transport in a method approved for classified information, unless this method is waived by the originating government.

9-6 TELEPHONE TRANSMISSION

Classified telephone conversations shall be permitted only over secure communication circuits approved for the classification level of the information being discussed. Every attempt shall be made to ensure that the classified information is not compromised to unauthorized personnel.

9-7 CLASSIFIED BULKY FREIGHT SHIPMENTS

Commanding officers shall establish procedures for shipping bulky classified information as freight. These procedures shall include provisions for shipment in closed vehicles when required, appropriate notice to the consignee concerning the shipment, procedures at transshipment activities, and actions to be taken in case of non-delivery or unexpected delay in delivery.

9-8 PREPARING CLASSIFIED INFORMATION FOR SHIPMENT

1. Prepare classified information for shipment by packaging and sealing it with tape which will retain the impression of any postal stamp, in ways that minimize risk of accidental exposure or undetected deliberate compromise. Classified information shall be packaged so that classified text is not in direct contact with the inner envelope or container.

17 MAR 1999

2. Enclose classified information transported outside the command in two opaque, sealed covers (e.g., envelopes, wrappings, or containers) durable enough to conceal and protect it from inadvertent exposure or tampering. The following exceptions apply:

a. If the classified information is an internal component of a packageable item of equipment, the outside shell or body may be considered as the inner cover provided it does not reveal any classified information.

b. If the classified information is an inaccessible internal component of a bulky item of equipment, the outside or body of the item may be considered a sufficient cover provided observation does not reveal classified information.

c. If the classified information is an item of equipment that is not reasonably packageable and the shell or body is classified, it shall be concealed with an opaque covering that conceals all classified features.

d. Specialized shipping containers, including closed cargo transporters, may be considered the outer wrapping or cover when used.

e. Refer to the appropriate reference in paragraph 9-5 for preparation of special types of classified and controlled unclassified information for transmission or transportation.

9-9 ADDRESSING CLASSIFIED INFORMATION FOR SHIPMENT

1. Address the outer envelope or container only to an official U.S. Government activity or a cleared DoD contractor facility with the appropriate FCL level and storage capability. Include the complete return address of the sender. The outer envelope or container shall not have any markings indicating, or alerting handlers to the classification level of the contents. The classified information shall not be addressed to an individual (except when using USPS Express Mail or the current holder of the GSA contract for overnight delivery); however, an attention line may be used to include an office code or a specific department to aid in internal routing. Classified information intended only for U.S. elements of international staffs or other organizations shall be addressed specifically to those elements.

17 MAR 1999

2. The inner envelope or container shall show the address of the recipient, the address of the sender, the highest classification level of the contents (including all warning notices, intelligence control markings, or any other applicable special instructions (see chapter 6, paragraphs 6-11 and 6-12)), and may also include an "attention line" with the intended recipient's name and/or office code.

3. Refer to the appropriate reference in paragraph 9-5 on addressing special types of classified and controlled unclassified information for transmission or transportation.

4. **DOS Diplomatic Courier Service.** The outer envelope of the classified information to be sent through the DOS Diplomatic Courier Service shall be addressed to: Chief, Classified Pouch and Mail Branch, U.S. Department of State, Washington, DC 20520-0528 and mailed via USPS registered mail. Mark the inner envelope with the appropriate classification level and address of the specific overseas activity.

5. **USPS Express Mail.** The USPS Express Mail envelope may serve as the outer wrapper.

6. **Current Holder of GSA Contract for Overnight Delivery.** The delivery envelope may serve as the outer wrapper and may be addressed to the recipient by name.

9-10 RECEIPTING FOR CLASSIFIED INFORMATION

1. Acknowledgement of receipt is required for Top Secret and Secret information transmitted or transported in and out of the command and for all classified information provided to a foreign government or its representatives, including its embassies in the U.S., and its contractors. A receipt is required with all classified packages handcarried to the U.S. Senate.

2. Use OPNAV 5511/10, Record of Receipt (exhibit 9B), and attach it to the inner cover. The receipt shall contain only unclassified information that clearly identifies the classified information. Retain Top Secret receipts for 5 years and Secret receipts for 2 years (see chapter 7, paragraph 7-7 for receipt retention of FGI). Failure to sign and return a receipt to the sender may result in a report of possible loss or compromise.

17 MAR 1999

**9-11 GENERAL PROVISIONS FOR ESCORTING OR HANDCARRYING
CLASSIFIED INFORMATION**

1. Use a cover sheet, file folder, or other covering to prevent inadvertent disclosure when handcarrying classified information within the command.
2. Double-wrap the classified information when handcarrying outside the command. A locked briefcase may serve as the outer cover, except when handcarrying aboard commercial aircraft. When handcarrying classified information to another command, refer to the provisions of this chapter on requirements for receipting, addressing, and covering.
3. Second echelon commands shall approve escorting or handcarrying of classified information aboard commercial aircraft traveling outside the U.S., its territories, and Canada. This authority may be further delegated, in writing, to subordinate commands as necessary.
4. Commanding officers or other designated officials shall authorize official travelers to escort or handcarry classified information only when:
 - a. The information is not available at the destination and is needed for operational necessity or a contractual requirement;
 - b. The information cannot be transmitted via a secure facsimile or other secure means in sufficient time for the stated purpose;
 - c. The escort or handcarry is accomplished aboard a U.S. carrier, or a foreign carrier if no U.S. carrier is available and the information remains in the custody and physical control of the U.S. courier or escort at all times; and
 - d. Advance arrangements have been made for secure storage at a U.S. embassy, military or cleared DoD contractor facility with safeguarding capability, commensurate with the classification level of the handcarried information, at the destination and all intermediate stops.
5. Commanding officers shall ensure that couriers are informed of and acknowledge their security responsibilities when escorting or handcarrying classified information. The latter requirement

SECNAVINST 5510.36

17 MAR 1999

may be satisfied by a briefing or by requiring the courier to read written instructions that contain the information listed below, as a minimum:

a. The courier is liable and responsible for the information being escorted;

b. The information is not, under any circumstances, to be left unattended;

c. During overnight stops, classified information is to be stored at a U.S. embassy, military or appropriately cleared DoD contractor facility (see paragraph 9-11.4d) and shall not, under any circumstances, be stored in vehicles, hotel rooms or safes;

d. The information shall not be opened enroute except in the circumstances described in subparagraph 9-11.5h;

e. The information shall not be discussed or disclosed in any public place or conveyance;

f. The courier shall not deviate from the authorized travel schedule;

g. The courier is responsible for ensuring that personal travel documentation (passport, courier authorization, and medical documents) are complete, valid, and current;

h. There is no assurance of immunity from search by security, police, customs and/or immigration officials on domestic or international flights. Carry-on bags and packages may be subjected to X-raying and inspection by customs or airline/airport security officials. If there is a question about the contents of the package, the courier shall present the courier authorization to the official or to the official's supervisor, if necessary. If the official demands to see the actual contents of the package, it may be opened in his or her presence, in an area out of sight of the general public. However, under no circumstances shall classified information be disclosed. Immediately after the examination, the courier shall request that the package be resealed and signed by the official to confirm that the package was opened. Inform both the addressee and the dispatching security officer in writing of the opening of the package;

17 MAR 1999

i. The courier shall carry a copy of an inventory of the contents in the sealed package and submit a copy to the courier's security office for retention;

j. Upon return, the courier shall return all classified information in a sealed package or furnish documentation signed by an authorized security official of the addressee organization for any information that is not returned;

k. Refer to reference (f) on the handcarry of classified NATO information.

6. In the event that the handcarry of classified information will also involve the disclosure of classified information to foreign nationals, the command foreign disclosure approving official shall ensure that disclosure authorization has been obtained per reference (o).

9-12 AUTHORIZATION TO ESCORT OR HANDCARRY CLASSIFIED INFORMATION

1. The Security Manager shall provide written authorization to all individuals escorting or handcarrying classified information. This authorization may be the DD 2501, Courier Authorization Card, or included on official travel orders, visit requests, or a courier authorization letter. Any of these four written authorizations may be used to identify appropriately cleared DoD military and civilian personnel approved to escort or handcarry classified information (except for SCI and SAP) between DoD commands per the following, except for travel aboard commercial aircraft, in which case the provisions of paragraph 9-13 also apply:

a. The individual has a recurrent need to escort or handcarry classified information;

b. The written authorization is signed by an appropriate official in the servicing security office;

c. The expiration date may not exceed 3 years from the issue date (pertains only to DD 2501);

d. Retrieve the written authorization upon an individual's transfer, termination of employment, or when authorization is no longer required;

e. When using the DD 2501, a limited number may be issued to "Bearer," on a case-by-case basis, to individuals who need to handcarry classified information for a specific event. In this

17 MAR 1999

instance, Item 2 on the card shall be annotated "Indefinite". The DD 2501 is controlled to preclude unauthorized use and local reproduction is prohibited.

2. The written authorization is intended for use between DoD commands worldwide and provides sufficient authorization to handcarry classified information aboard a U.S. military aircraft.

3. See appendix B for courier card procurement information.

**9-13 AUTHORIZATION LETTER FOR ESCORTING OR HANDCARRYING
CLASSIFIED INFORMATION ABOARD COMMERCIAL PASSENGER AIRCRAFT**

1. Personnel escorting or handcarrying classified information aboard commercial aircraft shall process through the airline ticketing and boarding procedures in the same manner as other passengers. Advance coordination shall be made with airline and departure terminal officials and, when possible, with intermediate transfer terminals to develop mutually satisfactory arrangements within the terms of this regulation and Federal Aviation Administration (FAA) guidance to facilitate the courier's processing through airline ticketing, screening, and boarding procedures. Local FAA field offices can often be of assistance. During this coordination, specific advice shall be sought regarding the nature of documentation that will be required. Generally, the following will meet commercial airline security requirements:

a. The individual designated as courier shall possess an identification card that includes a photograph, date of birth, height, weight, and signature. If the identification card does not contain these items they shall be included in the written authorization.

b. The courier shall handcarry the original authorization letter and sufficient copies to provide documentation to airline officials. Prepare the authorization letter on command letterhead authorizing transport of the classified information and include the following information:

(1) The full name of the individual and employing agency;

(2) Description of the personal identification the individual will present (e.g., VA Drivers License No. 1234);

(3) Description of material being carried (e.g., three sealed packages, 9" X 8" X 24"), addressee and sender;

17 MAR 1999

(4) The point of departure, destination, and known transfer points;

(5) A date of issue and expiration date;

(6) The name, title, and signature of the official issuing the letter. The official shall sign each package or carton on its face;

(7) The name and a valid U.S. Government telephone number of the official designated to confirm the courier authorization letter.

2. If a return trip is necessary, the host security official at the original destination shall conduct all necessary coordination and provide an endorsement to the original courier authorization letter to include the updated itinerary.

9-14 ESCORT OR HANDCARRY OF CLASSIFIED INFORMATION TO THE U.S. SENATE

1. Top Secret packages shall be handcarried to the Office of Senate Security, Room S-407, the Capitol. Other classified packages being handcarried directly to the U.S. Senate shall be by an authorized courier, to one of the following offices:

a. The Committee on Appropriations, Room SD-119, Dirksen Building;

b. The Committee on Armed Services, Room SR-228, Russell Building. This office will accept only receipted classified packages addressed to the Chairman, the Ranking Minority Member, or to individual Committee staff members. Classified packages addressed to all others shall be delivered to the office of Senate Security;

c. The Committee on Foreign Relations, Room SD-423, Dirksen Building; or

d. The Committee on Intelligence, Room SH-211, Hart Building.

2. Under no circumstances shall classified packages be delivered directly to a Senator's personal office.

3. Mail Secret and Confidential packages only by USPS registered mail, addressed to the Director, Office of Senate Security, Room S-407, The Capitol, Washington, D.C. 20510-7114.

SECNAVINST 5510.36

17 MAR 1999

4. Prepare the package per paragraphs 9-8 and 9-9 with the inner envelope addressed to the intended recipient (e.g., Senator, staff member, committee, subcommittee, or other Senate office). Include a multiple-copy receipt with all classified packages handcarried to the U.S. Senate.

REFERENCES

- (a) DoD 5200.33-R, *Defense Courier Service*, 7 Nov 94
- (b) *National Communications Security Instruction (NCSI) 4009, Protected Distribution Systems (U)*, 30 Dec 81
- (c) DoD 5220.22-M, *National Industrial Security Program Operating Manual (NISPOM)*, Jan 95 (NOTAL)
- (d) CMS-1A, *Cryptographic Security Policy and Procedures Manual (U)*, 25 Feb 98 (NOTAL)
- (e) CMS-21 Series, *Interim CMS Policy and Procedures for Navy Tier 2 Electronic Key Management System*, 30 May 97 (NOTAL)
- (f) OPNAVINST C5510.101D, *NATO Security Procedures (U)*, 17 Aug 82 (NOTAL)
- (g) DoD 5105.21-M-1, *DoD Sensitive Compartmented Information Administrative Security Manual*, 3 Aug 98 (NOTAL)
- (h) OPNAVINST S5460.4C, *Control of Special Access Programs Within the Department of the Navy (U)*, 14 Aug 81 (NOTAL)
- (i) OPNAVINST S5511.35K, *Policy for Safeguarding the Single Integrated Operational Plan (SIOP) (U)*, 1 Jul 98
- (j) OPNAVINST C8126.1A, *Navy Nuclear Weapon Security (U)*, 20 Dec 94 (NOTAL)
- (k) SECNAVINST 5720.42E, *DON Freedom of Information Act (FOIA) Program*, 5 Jun 91
- (l) NAVSEAINST C5511.32B, *Safeguarding of Naval Nuclear Propulsion Information (NNPI) (U)*, 17 Oct 79 (NOTAL)

17 MAR 1999

- (m) **OPNAVINST 5570.2, DoD Unclassified Controlled Nuclear Information (DoD UCNI), 11 Feb 93**
- (n) **DoD 5200.28, Security Requirements for Automated Information Systems (AIS), 21 Mar 88 (NOTAL)**
- (o) **SECNAVINST 5510.31B, Policy and Procedures for Control of Foreign Disclosure in the DON, 31 Dec 92**

17 MAR 1999

EXHIBIT 9A

TRANSMISSION OR TRANSPORTATION TO FOREIGN GOVERNMENTS

1. Classified information and/or material approved for release to a foreign government shall be transferred between authorized representatives of each government in compliance with the provisions of this exhibit. Each contract, agreement, or other arrangement that involves the release of classified material as freight to foreign entities shall either contain detailed transmission instructions or require that a separate transportation plan be approved by the appropriate DoD security and transportation officials and the recipient government before release. Transportation plan requirements are outlined in paragraph 9. (DoD TS-5105.21-M-3 provides guidance regarding SCI).
2. Classified information and/or material released directly to a foreign government representative shall be delivered or transmitted only to a person who has been designated, in writing, by the recipient government to sign for and assume custody and responsibility on behalf of the government (hereafter referred to as the "designated government representative"). This written designation shall contain assurances that such a person has a security clearance at the appropriate level and that the person shall assume full responsibility for the information on behalf of the foreign government. The recipient shall be required to execute a receipt regardless of the level of classification.
3. Classified material that is suitable for transfer by courier or postal service per this regulation, and that cannot be transferred directly to a foreign government's designated representative, shall be transmitted to:
 - a. An embassy, consulate, or other official agency of the recipient government having extra-territorial status in the U.S.; or
 - b. A U.S. embassy or U.S. military organization in the recipient country or in a third party country for delivery to a designated representative of the recipient government.
4. The shipment of classified material as freight via truck, rail, aircraft, or ship shall be per the following:
 - a. The DoD officials authorized to approve a Foreign Military Sales (FMS) transaction that involves the delivery of

17 MAR 1999

U.S. classified material to a foreign purchaser shall, at the outset of negotiation or consideration of a proposal, consult with DoD transportation authorities (MTMC, Military Sealift Command, Air Mobility Command, or other authority, as appropriate), to determine whether secure shipment from the CONUS point of origin to the ultimate foreign destination is feasible. Normally, the U.S. shall use the Defense Transportation System (DTS) to deliver classified material to the recipient government. A transportation plan shall be developed by the DoD component that prepares the Letter of Offer and Acceptance (LOA) in coordination with the purchasing government. Security officials of the DoD component that prepares the LOA shall evaluate the adequacy of the transportation plan.

b. Classified shipments resulting from direct commercial sales shall comply with the same security standards that apply to FMS shipments. To develop and obtain approval of the required transportation plan, cleared DoD contractors shall consult with the purchasing government and the DSS Regional Operating Location (OPLOC) before consummation of a commercial contract that will result in the shipment of classified material.

c. Delivery of classified material to a foreign government at a point within the U.S. and its territories shall be accomplished at:

(1) An embassy, consulate, or other official agency under the control of the recipient government;

(2) The point of origin. When a designated representative of the recipient government accepts delivery of U.S. classified material at the point of origin (for example, a manufacturing facility or depot), the DoD official who transfers custody shall ensure that the recipient is aware of secure means of onward movement of the material to its final destination, consistent with the approved transportation plan;

(3) A military or commercial Port of Embarkation (POE) that is a recognized point of departure from the U.S. and its territories for on-loading aboard a ship, aircraft, or other carrier. In these cases, the transportation plan shall provide for U.S.-controlled secure shipments to the CONUS transshipment point and the identification of a secure storage facility, government or commercial, at or near the POE. A DoD official authorized to transfer custody shall supervise or observe the on-loading of FMS material being transported when physical and security custody of the material has yet to be transferred

17 MAR 1999

formally to the foreign recipient. In the event that transfer of physical and security custody cannot be accomplished promptly, the DoD official shall ensure that the classified material is either returned to a secure storage facility of the U.S. shipper (government or contractor); segregated and placed under constant surveillance of a duly cleared U.S. security force at the POE; or held in the secure storage facility designated in the transportation plan;

(4) An appropriately cleared freight forwarder facility identified by the recipient government as its designated representative. In these cases, a person identified as a designated government representative shall be present to accept delivery of the classified material and receipt for it, to include full acceptance of security responsibility.

5. Delivery outside the U.S. and its territories:

a. U.S. classified material delivered to a foreign government within the recipient country shall be delivered on arrival in the recipient country to a U.S. Government representative who shall arrange for its transfer to a designated representative of the recipient government. If the shipment is escorted by a U.S. Government official authorized to accomplish the transfer of custody, the classified material may be delivered directly to the recipient government's designated representative upon arrival.

b. U.S. classified material to be delivered to the representatives of a foreign government within a third country shall be delivered to an agency or installation of the U.S. or the recipient country which has extra-territorial status or is otherwise exempt from the jurisdiction of the third country. Unless the classified material is accompanied by a U.S. Government official authorized to accomplish the transfer of custody, a U.S. Government official shall be designated locally to receive the shipment upon arrival and deliver it to the recipient government's designated representative.

6. Overseas shipments of U.S. classified material shall be made only via ships, aircraft, or other carriers that are:

a. Owned or chartered by the U.S. Government or under U.S. registry;

b. Owned or chartered by or under the registry of the recipient government; or

17 MAR 1999

c. Otherwise authorized by the head of the DoD component having classification jurisdiction over the classified material involved. Overseas shipments of classified material shall be escorted, prepared for shipment, packaged, and stored aboard as prescribed elsewhere in this regulation and in DoD 5220.22-M.

7. Only freight forwarders that have been granted an appropriate FCL by the DoD or the recipient government are eligible to receive, process related security documents, and store U.S. classified material authorized for release to foreign governments. However, a freight forwarder that does not have access to or custody of the classified material, and is not required to perform security-related functions, need not be cleared.

8. Foreign governments may return classified material to a U.S. contractor for repair, modification, or maintenance. At the time the classified material is initially released to the foreign government, the approved methods of return shipment shall be specified in the LOA for FMS material, the security requirements section of a direct commercial sales contract, or in the original transportation plan. The contractor, upon notification of a return shipment, shall give advance notice of arrival to the applicable cognizant contracting command or the DSS and arrange for secure inland shipment within the U.S. if such shipment has not been prearranged.

9. Transportation plan requirements:

a. Preparation and coordination:

(1) FMS. U.S. classified material to be furnished to a foreign government or international organization under FMS transactions shall normally be shipped via the DTS and delivered to the foreign government within its own territory. The U.S. Government may permit other arrangements for such shipments when it determines that the recipient foreign government has its own secure facilities and means of shipment from the point of receipt to ultimate destination. In any FMS case, the DoD component having security cognizance over the classified material involved is responsible, in coordination with the foreign recipient, for developing a transportation plan. When the point of origin is a U.S. contractor facility, the contractor and DSS shall be provided a copy of the plan by the DoD component.

17 MAR 1999

(2) Commercial Transactions. The contractor shall prepare a transportation plan for each commercial contract, subcontract, or other legally binding arrangement providing for the transfer of classified freight to foreign governments, to be moved by truck, rail, aircraft, or ship. The requirement for a transportation plan applies to U.S. and foreign classified contracts. The DSS will approve transportation plans that support commercial arrangements or foreign classified contracts.

(3) The transportation plan shall describe arrangements for secure shipment of the classified material from the point of origin to the ultimate destination. It shall identify recognized POEs from the U.S. and its territories for transfer to a specified ship, aircraft, or other authorized carrier. It shall identify a government or commercial secure facility in the vicinity of the POEs and debarkation that can be used for storage if transfer or onward movement cannot take place immediately. Except as described in paragraph 9a(4), a U.S. Government official authorized to transfer custody and control shall supervise the on-loading of classified material when it has yet to be officially transferred. The plan shall provide for security arrangements in the event custody cannot be transferred promptly.

(4) Upon transfer of the title to the purchasing foreign government, classified material may be delivered to a freight forwarder that is designated, in writing, by the foreign government as its representative for that shipment and is cleared to the level of the classified information to be received. The freight forwarder shall be provided a copy of the transportation plan and agree to comply.

b. The transportation plan shall, as a minimum, include:

(1) A description of the classified material to be shipped and a brief narrative describing where and under what circumstances transfer of custody will occur;

(2) Identification, by name and title, of the designated government representative (or alternate) of the recipient government or international organization who will receipt for and assume security responsibility;

(3) Identification and specific location(s) of delivery point(s) and security arrangements while located at the delivery point(s);

17 MAR 1999

(4) Identification of commercial carriers and freight forwarders or transportation agents who will be involved in the shipping process, the extent of their involvement, and their clearance;

(5) Identification of any storage or processing facilities and transfer points to be used; certification that such facilities are authorized by competent government authority to receive, store, or process the level of classified material to be shipped; and a description of security arrangements while located at the facilities;

(6) Routes and, if applicable, security arrangements for overnight stops or delays enroute;

(7) Arrangements for dealing with port security and customs officials;

(8) The identification, by name or title, of couriers, escorts, or other responsible officials (e.g. captain or crew chief) to be used, including social security number, government identification, or passport number, security clearance, and details concerning their responsibilities;

(9) Description of the shipping methods to be used and the identification of the foreign or domestic carriers;

(10) Description of packaging requirements, seals, and storage during shipment;

(11) A requirement for the recipient government or international organization to examine shipping documents upon receipt in its own territory; and a requirement to notify DSS or the DoD component having security cognizance if the information has been transferred enroute to any carrier not authorized by the transportation plan;

(12) Requirement for the recipient government or international organization to inform DSS or the DoD component having security cognizance over the classified information promptly and fully of any known or suspected compromise of the classified information;

(13) Arrangements for return shipments, if necessary for repair, modification, or maintenance.

17 MAR 1999

EXHIBIT 9B

RECORD OF RECEIPT
(OPNAV 5511/10)OPNAV 5511/10 (Rev 12-89)
S/N 0107-LF-008-8000RECORD OF RECEIPT
(REFERENCE OPNAVINST 5510.1M)THIS RECEIPT MUST BE
SIGNED AND RETURN

ORIGINATOR'S CODE	FILE OR SERIAL NO.	DATE OF MATERIAL	UNCLASSIFIED DESCRIPTION	COPY NO.	NO. OF ENCLS TO MAT'L REC'D
N09N2	12345	(Date)	Security Classification Guide	1	1

ADDRESSEE (Activity Receiving Material)

REGISTERED NUMBER

CNO (N09N2)

SIGNATURE (Authorized Receipt)

R.W. MARSHALL

R.W. Marshall

DATE

20 OCT 98